



SHARKFEST '14
WIRESHARK DEVELOPER AND USER CONFERENCE
JUNE 16-20 2014 · DOMINICAN UNIVERSITY

Common Mistakes in Packet Analysis

Things that make traces harder to read.

Chris Greer, Network Analyst
Packet Pioneer LLC

Presenter



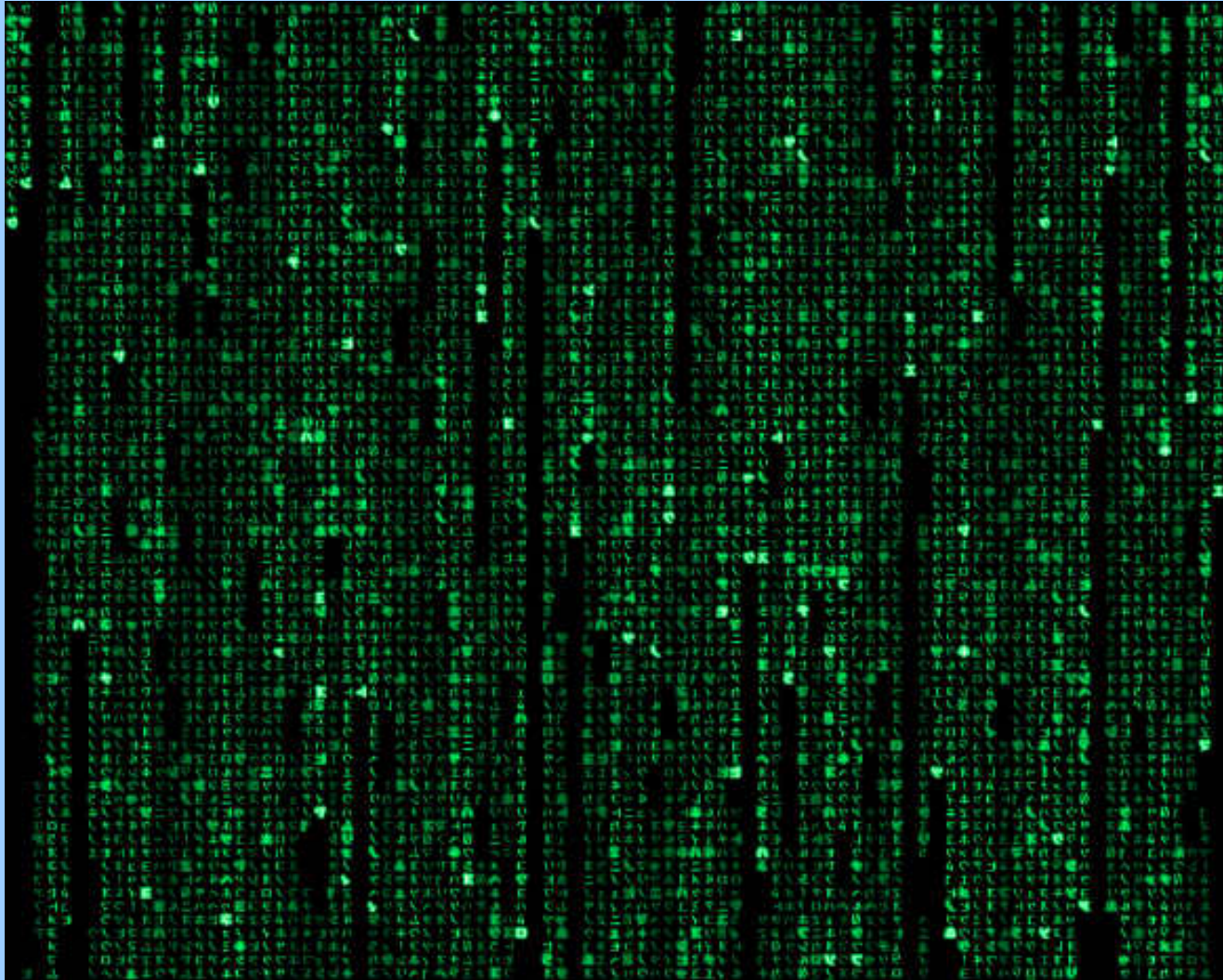
- Chris Greer
 - Packet Pioneer LLC
 - Focused on Network and Application Performance Analysis
 - Protocol Analysis Consulting
 - Deliver training focused on Wireshark, Fluke Networks, other vendors.

Why do I care?

- When analyzing complex problems, every packet counts



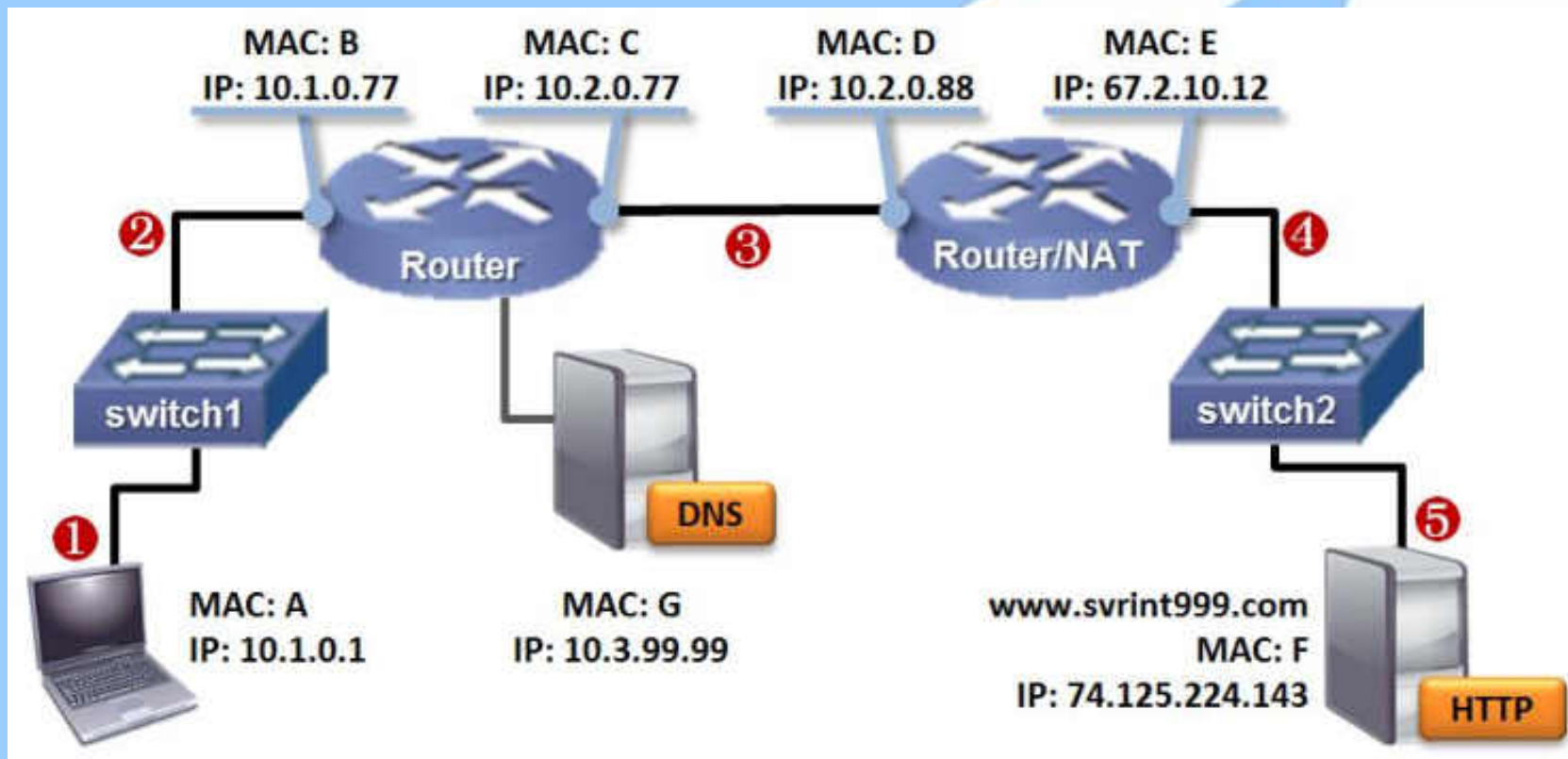
Why is it hard?



Or it can look like this...



1. Initially Capturing Too Much Traffic



Trace File Size



- File size at 1Gbps for 5 minutes, 50% utilization
~18GB file – approx 300 million packets
(512 Byte packet average)
- File size for 10Gbps for 5 minutes, 50% util
~180GB file – approx 3 billion packets!

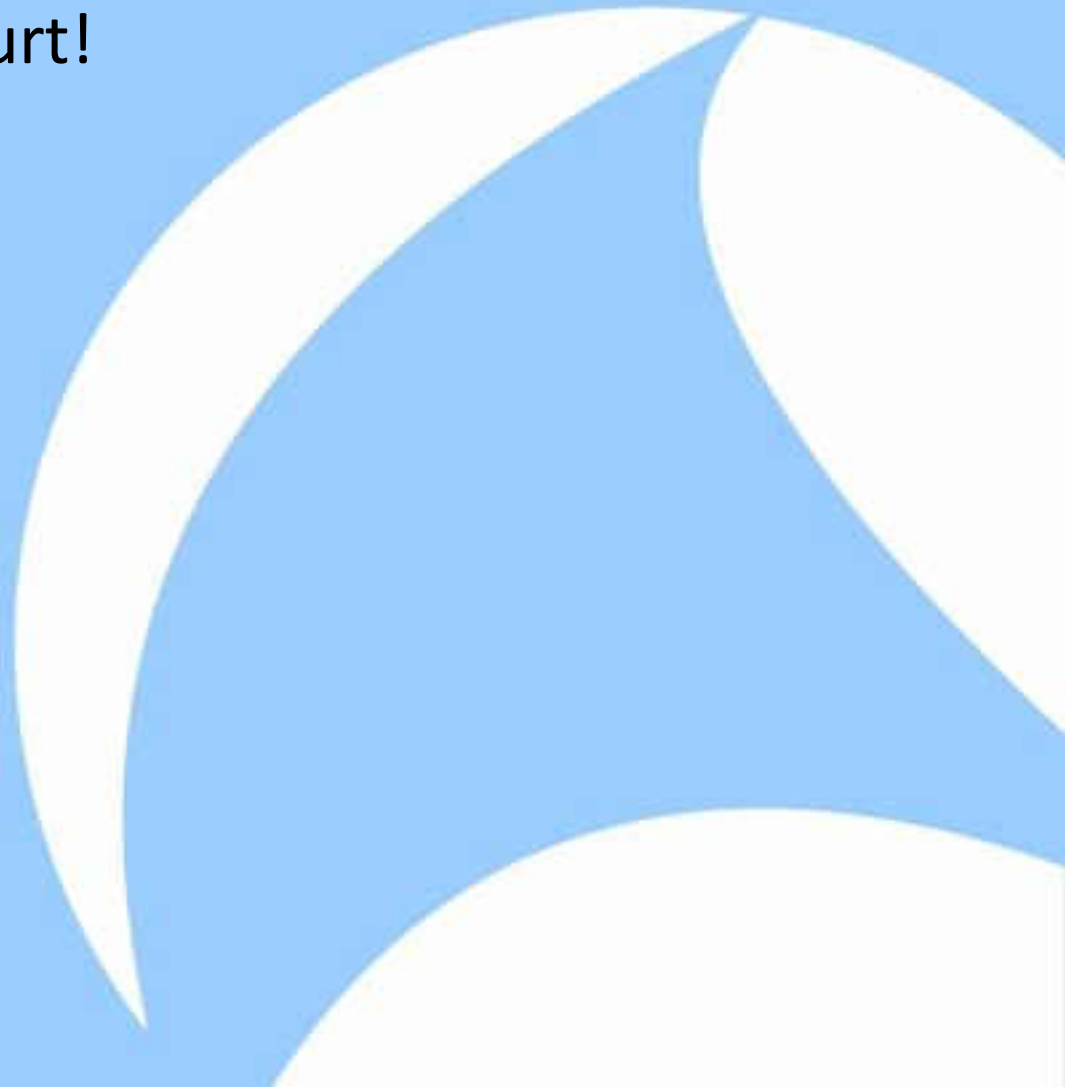
Packet Overload



- Even with filtering, locating the root cause of a problem can be overwhelming
- Start small – start at the client if you can

1. Capturing Too Much Traffic

- Large Trace Files can hurt!

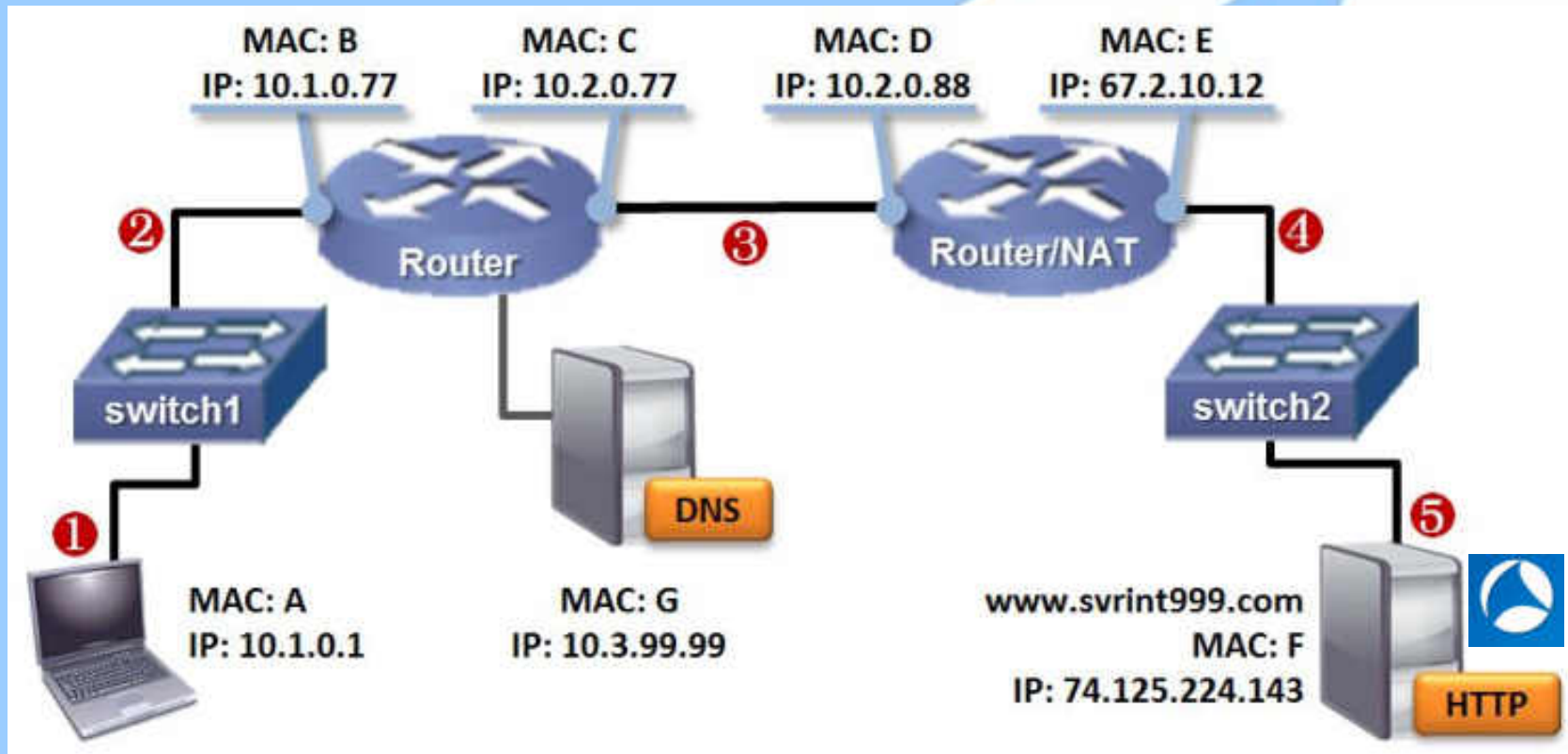


2. Not Thinking Before Capturing

- Think before you capture
 - What is the goal?
 - What is “it” that we are capturing?
 - Where do those packets flow?
- Capturing a problem doesn't mean we can interpret it



3. Capturing Locally on a System



3. Capturing Locally - Problems

- False Alarms with TCP
 - TCP Checksum Errors

```
Info
HTTP/1.1 200 OK
Continuation or non-HTTP traffic
Continuation or non-HTTP traffic
hbc i > 62227 [FIN, ACK] Seq=219 Ack=225 win=16640 [TCP CHECKSUM INCORRECT] Len=0
Continuation or non-HTTP traffic
hbc i > 62213 [FIN, ACK] Seq=219 Ack=438 win=16800 [TCP CHECKSUM INCORRECT] Len=0
Continuation or non-HTTP traffic
hbc i > 50948 [FIN, ACK] Seq=219 Ack=225 win=16640 [TCP CHECKSUM INCORRECT] Len=0
Continuation or non-HTTP traffic
hbc i > 52830 [FIN, ACK] Seq=219 Ack=225 win=16640 [TCP CHECKSUM INCORRECT] Len=0
Continuation or non-HTTP traffic
hbc i > 62219 [FIN, ACK] Seq=219 Ack=225 win=16640 [TCP CHECKSUM INCORRECT] Len=0
Continuation or non-HTTP traffic
hbc i > 62217 [FIN, ACK] Seq=219 Ack=225 win=16640 [TCP CHECKSUM INCORRECT] Len=0
```

3. Capturing Locally - Problems

- Things may look “weird”
- Example – 16,000 byte packets.
- Strange timing issues (0.000000 deltas)

3. Capturing Locally - Problems

- Non-dedicated capture hardware will have a limit!



Wireshark Downloads

- Estimated at 500,000 per month – Wireshark Network Analysis Study Guide
- How many of these downloads are to laptops?
- How many of these users leave the optimization settings at the default rate?

- Very likely – MOST!

Laptops have a purpose

- Email, Web, Work Applications, Music Players, etc...
- Make their owners mostly happy
- Network Analysis is not the purpose of most laptops



Is 1Gig really capturing at 1Gig?

- A laptop likely has a 1Gig interface. Does that mean that it can capture traffic at that rate?
- Most of us agree – no.
- So, when does it start dropping packets?
- At what utilization point do we really need to consider a hardware-based appliance?

1001101001010010101011001001000111010



Capture limitation on default settings



Aggregation Switch

This is not emulated traffic – it is an easily configurable packet generator.

Capture Limit Results

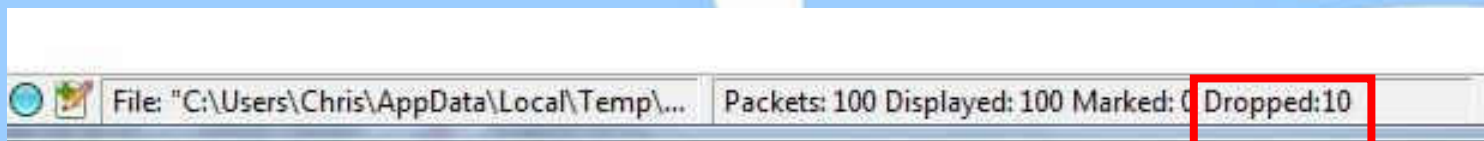
- Dell XPS 15z – i7 – 8GB Ram
 - Consistently can capture 80Mbps
- It's not much better on other systems.

What do dropped packets look like?

- Expert Info:
 - Previous Segment Lost
 - ACKed Lost Packet
 - Out of Order

102	o	0.705892	192.168.1.2	192.168.1.1	TCP	170	msg-icp > 65469 [PSH, ACK] Seq=2601 Ack=2133 Win=8256 Len=104 TSval=17356922 TSecr=16556
103	o	0.705892	192.168.1.1	192.168.1.2	TCP	66	65469 > msg-icp [ACK] Seq=2133 Ack=2705 Win=17416 Len=0 TSval=16556 TSecr=17356921
104	o	0.705892	192.168.1.2	192.168.1.1	TCP	170	msg-auth > 65523 [PSH, ACK] Seq=2601 Ack=2133 Win=8256 Len=104 TSval=17356923 TSecr=343424
105	o	0.775881	192.168.1.1	192.168.1.2	TCP	230	[TCP ACKed unseen segment] [TCP Previous segment not captured] 65523 > msg-auth [PSH, ACK]
106	•	0.776881	192.168.1.1	192.168.1.2	TCP	230	[TCP ACKed unseen segment] [TCP Previous segment not captured] 65469 > msg-icp [PSH, ACK]

- Dropped Counter

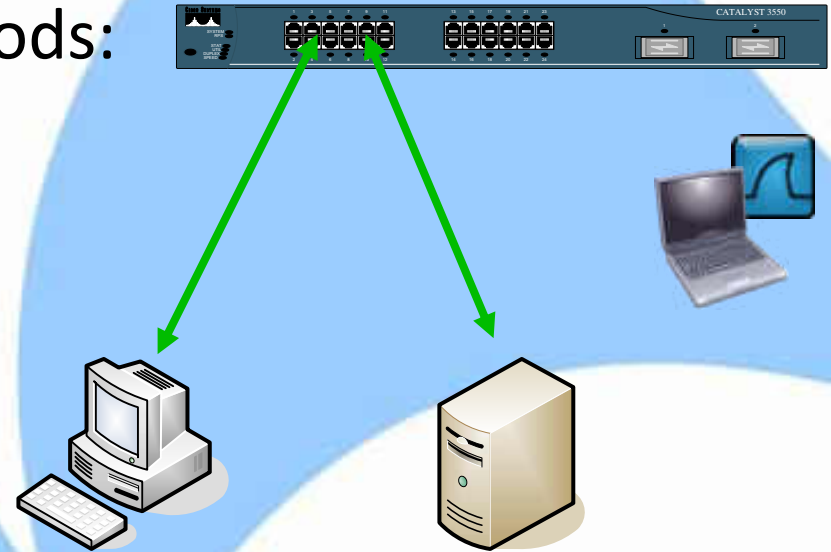


4. Switches (and Virtualization) make capturing difficult

- A packet is only forwarded to the destination port
- In order to capture it, the analyzer must be inline somewhere

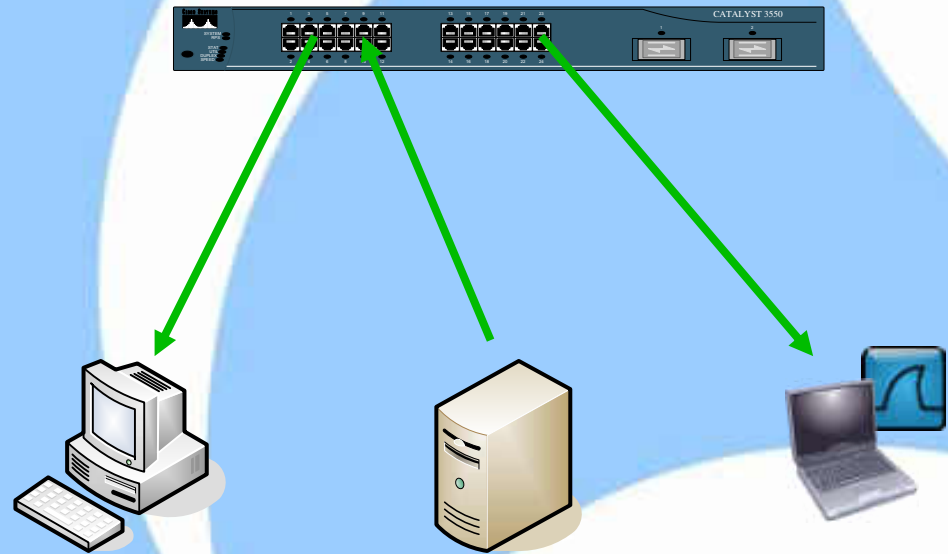
- 3 common capture methods:

- Hub
- Span/Mirror
- Tap



Getting in the path: Span/Mirror

- Copies selected ports, hosts, vlans, or traffic patterns to a monitor port



Getting in the path: Span/Mirror

- Pros

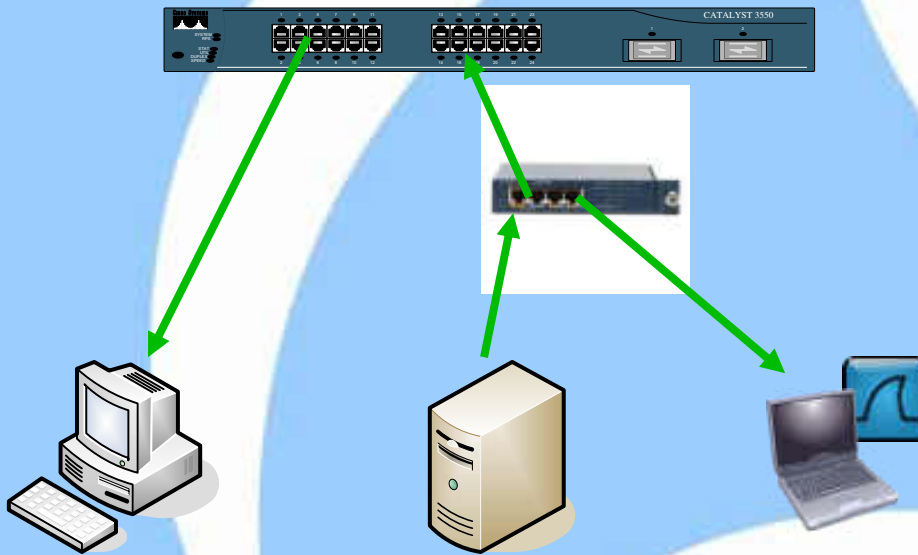
- Most switches already support it
- Free
- No need to break a link to configure it
- Full-duplex traffic analysis

- Cons

- Needs configuration
- Can't transmit back into the switch
- Easy to overload if monitoring many ports
- Requires documentation

Getting in the path: Taps

- A tap is the best means to capture packets
- Directly monitors the connection inline



Getting in the path: Taps

- Pros

- True inline analysis
- Full-Duplex
- No config necessary
- Power-fault tolerant
- Always available for capturing

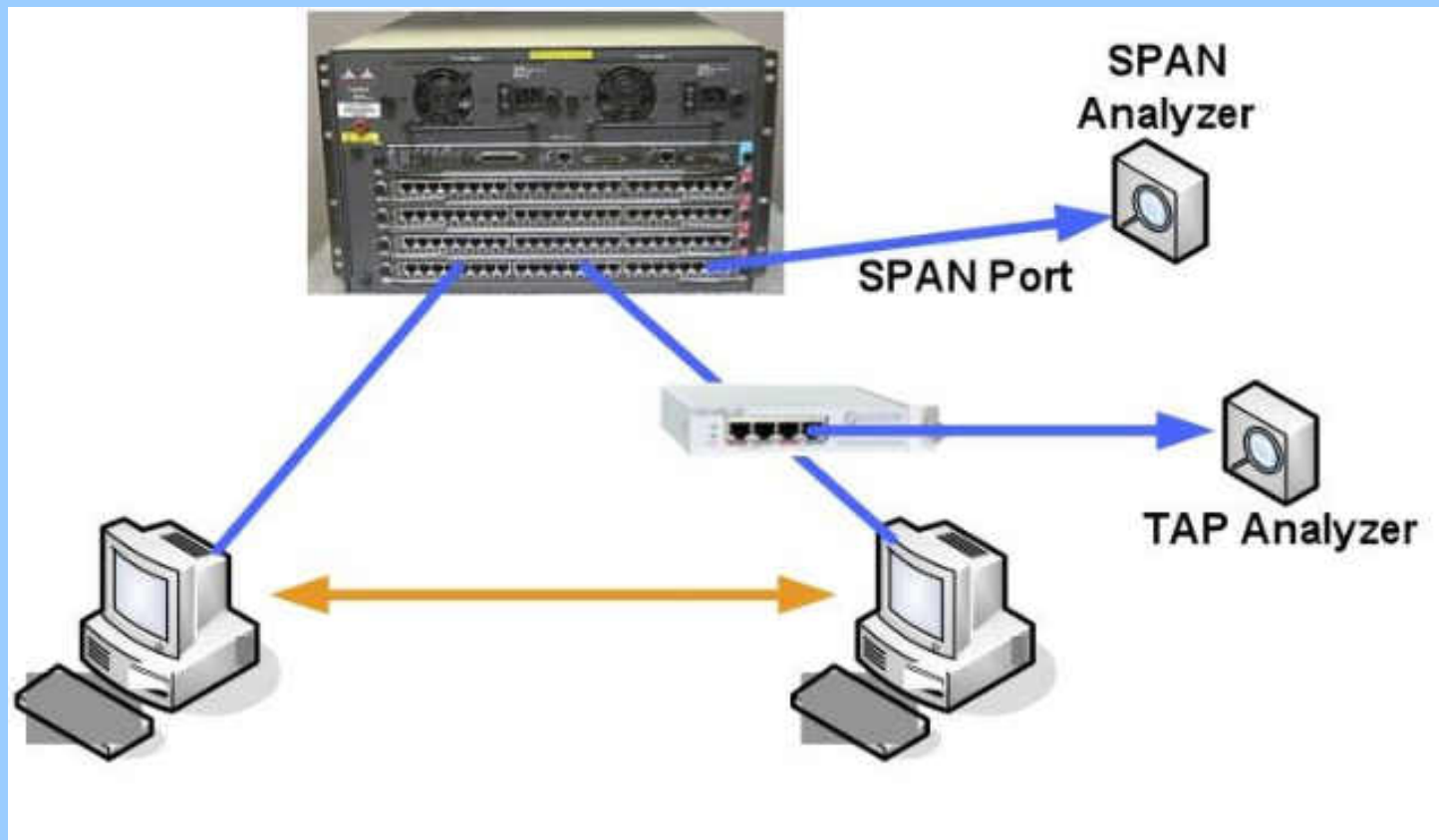
- Cons

- High cost compared to hub and span
- Need to break link the first time it is installed
- Harder to obtain

Overprovisioning doesn't only affect laptops

- Capture methods are affected too.
- A SPAN or Mirror port can be overprovisioned
- Especially when spanning a full VLAN or several gigabit ports at one time

SPAN/Mirror Example



SPAN vs. Tap Results

- Tap Capture Results
- Packets captured: 133,126
Delta Time at TCP Setup: 243uSec
- SPAN Capture Results
- Packets captured: 125,221
Delta time of TCP connection setup: 221 uSec

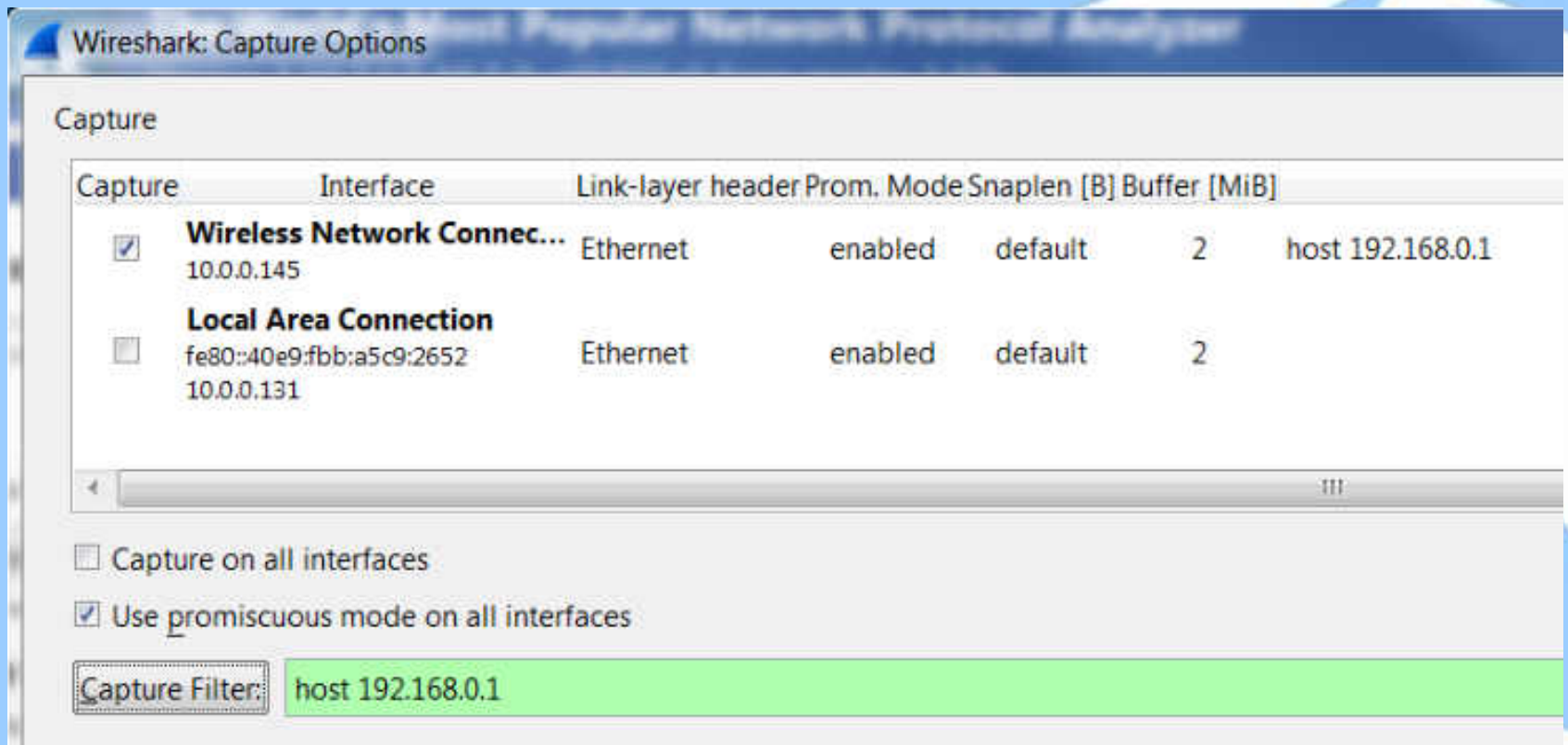
Hardware Based Capture

- Designed to capture at full line rate up to 10Gbps
- Stream to disk with no gaps or drops
- TurboCap NIC from Riverbed




- Cascade Appliance from Riverbed

5. Forgetting Capture Filters

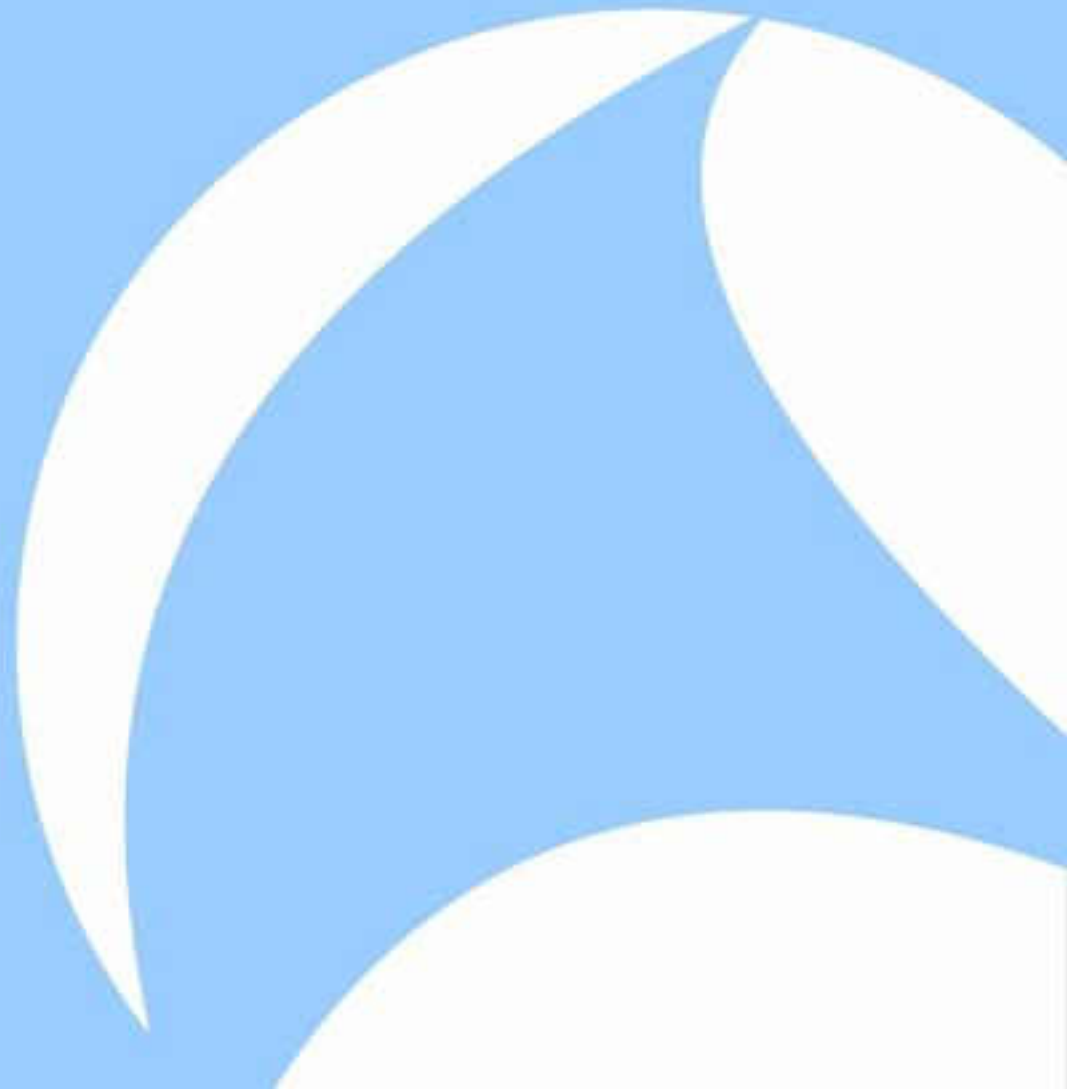


6. Wireshark Not Configured to Your

- Too many columns
 - Too few columns
 - Coloring rules that you don't understand
- 

7. Taking the Expert Info as gospel

- TCP Checksum errors
- TCP Port Reused



8. Packet-Level distractions

- Allowing packets that are not related to the root issue to distract attention





Thanks!

Common Mistakes in Packet Collection

Chris Greer, Network Analyst
Packet Pioneer LLC